AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Currently Amended) A secure method of transmitting a message between a sender node and a recipient node within a network collaboration group, the sender node and the recipient node sharing a secret encryption key and an expected nonce value comprising:

generating a new nonce value known to the sender node;

encrypting the message, ~~including~~ the expected nonce value and the new nonce value, using the encryption key, to create an encrypted message;

transmitting the encrypted message from the sender node to the recipient node; and

verifying, by the recipient node, that the encrypted message includes the expected nonce value, where the expected nonce value and the new nonce value are recoverable from the encrypted message using only knowledge possessed by the recipient node prior to receipt of the encrypted message.

2. (Currently Amended) The method of claim 1, further comprising:

generating a second new nonce value, known to the recipient node;

transmitting a secure response from the recipient node to the sender node by repeating the method of claim 1, but this time using the second new nonce value in place of the new nonce value and using the new nonce value in place of the expected nonce value.

3. (Currently Amended) The method of claim 2, wherein the method is further repeated for one or more subsequent rounds of secure communication between the sender node and the recipient node, such that for each round the new nonce value of

the previous message is used as the expected nonce value for the current message.

4. (Original) The method of claim 1, wherein the network collaboration group is a virtual private network.

5. (Currently Amended) The method of claim 1, wherein the sender node is a key managing master node and the recipient node is a member node of the collaboration group.

6. (Currently Amended) The method of claim 1, wherein the recipient node is a key-managing master node and the sender node is a member node of the collaboration group.

7. (Currently Amended) The method of claim 1, wherein ~~the method is used with~~ one of the sender node and the recipient node is a key-managing master node ~~in order to perform~~ that performs an authentication process for opening a collaboration group session with a new member node, the new member node being the other of the sender node and the recipient node.

8. (Currently Amended) The method of claim 7, wherein the method is used with the new member node as the sender node and the master node as the recipient node, in order to initiate the authentication process.

9. (Currently Amended) The method of claim 7, wherein the method is used with the master node as the sender node in order to distribute a session encryption key from the master node to the new member node.

10. (Currently Amended) The method of claim 9, wherein a long-term password key is used as the encryption key in order to perform the authentication process, and the session key is used as the encryption key for one or more subsequent communications

between the new member node and the master node.

11. (Currently Amended) The method of claim 10, wherein the session key is revoked by the master node upon receipt of a termination message from the new member node.

12. (Original) The method of claim 1, further including receiving a copy of a prior message being transmitted as a replay attack, and rejecting the replay as illicit at least in part because the replay does not contain the current expected nonce value.

13. (Currently Amended) A system for managing communications within a network collaboration group, comprising:

means for generating a new nonce value;

means for incorporating a message, an expected nonce value and the new nonce value in ~~a message to be transmitted~~ an encrypted message;

~~means for encrypting the message;~~

means for transmitting the encrypted message from a sender node of the group to a recipient node of the group; and

means for verifying, by the recipient node, that the encrypted message includes the expected nonce value, where the expected nonce value and the new nonce value are recoverable from the encrypted message using only knowledge possessed by the recipient node prior to receipt of the encrypted message.

14. (Currently Amended) The system of claim 13, wherein the means for incorporating are operable to use the new nonce value, contained in a most recent previous message from the sender node to the recipient node, as the expected nonce value in a current message from the recipient node to the sender node.

15. (Original) The system of claim 13, wherein the network collaboration group is a virtual private network.

16. (Currently Amended) A data-carrying signal for transmitting information securely between a master node and a member node of a network collaboration group, the signal being encrypted using an encryption key shared by the master node and the member node, the signal comprising:

the information to be transmitted;

an expected nonce value known to the master node and the member node; and

a new nonce value, different than the expected nonce, provided by a sender of the signal, the sender being one of the master node and the member node, where the expected nonce value and the new nonce value are recoverable from the signal using only knowledge possessed by a recipient node prior to encryption of the signal, the recipient node being one of the master node and the member node that did not send the signal.

17. (Currently Amended) The data-carrying signal of claim 16, wherein the expected nonce value in the current transmission is obtained from the new nonce value contained in a most recent previous transmission from the sender node to the recipient node.

18. (Currently Amended) A method for transmitting secure messages between a master node and a member node of a network collaboration group comprising:

encrypting-messages using a key shared by the master node and the member node, so as to protect confidentiality of the message; and

embedding a plurality of updated nonce values within said encrypted messages so as to provide verifiable integrity, authenticity, and freshness for each of said messages, where said plurality of updated nonce values are recoverable from the messages using only knowledge possessed by the recipient node prior to said encrypting, said recipient node being one of the master node and the member node that receives the encrypted messages.